IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Confirmation Number: 2845
Williamson, *et al.*	Group Art Unit: 2435
Serial No.: 10/687,694	Examiner: Moran, Randal D.
Filed: October 20, 2003	Docket No.: 200207546-3

For: Propagation of Viruses Through an Information Technology Network

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed herewith, responding to the final Office Action mailed August 24, 2009.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1 – 43 stand finally rejected. No claims have been allowed. The final rejections of claims 1 – 43 are appealed.

IV. Status of Amendments

No amendments have been made or requested since the mailing of the Final Office Action and all amendments submitted prior to the Final Office Action have been entered. The claims in the attached Claims Appendix (see below) reflect the present state of the pending claims.

V. Summary of Claimed Subject Matter

The claimed subject matter is summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter

described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host: establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host; during a first time interval (page 20, line 10, page 22, line 28, and originally filed claim 1), comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record; transmitting all requests to send data (page 22, line 28 and originally filed claim 1); and storing in a buffer data relating to requests which identify a destination host not in the record (page 23, line 28 and originally filed claim 1).

Embodiments according to independent claim 29 describe a method of operating a first host within a network of a plurality of hosts, the method comprising the following steps carried out by a first host: over the course of a first time interval, monitoring creation of sockets within the first host to identify destination hosts identified therein (page 9, line 22 and originally filed claim 29); comparing identities of destination hosts monitored during the first time interval with destination host identities in a record (page 22, line 28 and originally filed claim 29); and storing data from all sockets which identify monitored destination hosts not in the record (page 23, line 28 and originally filed claim 29).

Embodiments according to independent claim 43 describe a method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host: establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host (page 20, line 10, page 22, line 28, and originally filed claim

43); during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record; transmitting all requests to send data (page 22, line 28 and originally filed claim 43); and based on the result of the comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record (page 23, line 28 and originally filed claim 43).

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1 – 6, 8, 9, 14 – 18, 20, 21, 23, 28 – 35, 38, and 41 – 43 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*").

Claim 7 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"), in view of U.S. Patent Number 7,058,974 ("*Maher*").

Claims 10 – 13 and 24 – 27 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") U.S. Patent Number 5,341,491 ("*Ramanujan*").

Claims 19 and 22 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") E.P. Patent Number EP 0 986 229 ("*Cunningham*").

Claims 36, 37, 39, and 40 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") U.S. Patent Number 2002/0013858, Andersen ("*858*").

VII. Arguments

Appellant respectfully submit that pending claims 1 – 43 are patentable under 35 U.S.C. §103. Appellants respectfully request that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. The Cited References

1. The *Andersen* Reference

Andersen discloses a "method and apparatus for remote network access logging and reporting intercepts an access request at a client system on a network and sends log data identifying the access request to a log server on the network" (Abstract).

2. The *Shipp* Reference

Shipp discloses a "system for processing emails [that] incorporates means for dealing with previously unknown viruses" (Abstract).

3. The *Adolph* Reference

Adolph discloses "generation of data by mobile units (vehicles) to model reality concerning route(s) and traffic, and storing this data for further use" (Abstract).

4. The *Maher* Reference

Maher discloses "scanning the contents of the data packets flowing over the data network using a traffic flow scanning engine" (Abstract).

5. The *Ramanujan* Reference

Ramanujan discloses a "lockout avoidance circuit is provided for a plurality of nodes which generate lock requests for a shared resource such as a memory location" (Abstract).

6. The *Cunningham* Reference

Cunningham discloses a "method and system for monitoring and controlling network access [that] includes non-intrusively monitoring network traffic and assembling data packets that are specific to individual node-to-node transmissions in order to manage network access both inside and outside of a network" (Abstract).

7. The *858* Reference

'858 discloses "reducing data transmissions, especially ARP broadcast and response transmissions, within a computer network" (Abstract).

B. Rejections Under 35 U.S.C. §103

1. Claim 1 is Allowable Over *Andersen, Shipp,* and *Adolph*

The Office Action indicates that claim 1 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"). Appellants respectfully traverse this rejection for at least the

reason that *Andersen* in view of *Shipp* and *Adolph* fail to disclose, teach, or suggest all of the elements of claim 1. More specifically, claim 1 recites:

> A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:
> ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***;
> during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;
> transmitting all requests to send data; and
> ***storing in a buffer data relating to requests which identify a destination host not in the record***.
> ***(Emphasis added).***

Appellants respectfully submit that claim 1 is allowable over the cited art for at least the reason that none of *Andersen*, *Shipp*, and *Adolph*, taken alone or in combination, discloses, teaches, or suggests a "method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host... ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***... [and] ***storing in a buffer data relating to requests which identify a destination host not in the record***" as recited in claim 1. First, as previously argued, the combination of references simply does not teach "***storing in a buffer data relating to requests which identify a destination host not in the record***." The Office Action has repeatedly argued that *Shipp* and *Andersen* must be considered. Appellants submit that even a combination of *Shipp* and *Andersen* fail to render claim 29 obvious. More specifically, *Shipp* clearly discloses a "logger 22 [that] is programmed so that the system logs components of each message so that similar messages can be detected. The following are logged: Subject line and digest of subject line; First few characters of text

part of email, digest of first text part, and digest of first few characters..." (page 10, line 21). *Shipp* continues, disclosing:

> [t]he stopper 25 takes signatures from the searcher 24. The signature identifies characteristics of emails which must be stopped. On receiving the signature, all future matching emails are treated as viruses, and stopped. Obviously, the stopping action can take a number of forms, including... Holding them in temporary storage and notifying the addressee by email that an infected message has been intercepted and is being held for a period for their retrieval, should they wish, otherwise it will be deleted.
>
> (Page 11, line 30).

As clearly illustrated in this passage, *Shipp* is identifying characteristics of the email message to determine whether to "hold them in temporary storage." *Andersen* however, discloses an "identifier of the host system being accessed, for example the URL of the host system being accessed, may be extracted from the request and be included as the log data to be forwarded to log server 150 of FIG. 1" (column 5, line 19). Because *Shipp* is clearly and exclusively identifying characteristics of the email message to determine whether to "hold them in temporary storage," *Shipp* has no use for an extracted URL, as disclosed in *Andersen*. Consequently, the combination of references could not have suggested the teachings of claim 29.

Similarly, the cited references fail to suggest "***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***" as recited in claim 1. More specifically, the Office Action admits "[t]he combination [of *Andersen* and *Shipp*] does not explicitly disclose establishing a record which is at least indicative of identities of hosts within the network to whom data has been sent by a first host" (FOA page 4, line 18). Additionally, *Adolph* fails to overcome this deficiency. More specifically, *Adolph* discloses "[g]eneration of data by mobile units (vehicles) to model reality concerning route(s) and traffic and storing this data for further use" (Abstract). The portion of *Adolph* cited by the Office

action includes citation of Denmark Patent No. 38 28 725 A1, which describes "a method to record and sort a route carried out for the first time with a facility installed in the subject vehicle" (column 1, line 40). As illustrated in this passage, *Adolph* does not even suggest a "method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host... ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***" as recited in claim 1.

Further, *Adolph* discloses a "method and device for generating, merging, and updating of destination [vehicle] traffic data" (title), which is completely different than a "method and apparatus for remote network access logging and reporting" (*Andersen* title) or "monitoring e-mail traffic for viruses (*Shipp* title). More specifically, monitoring traffic data has nothing to do with monitoring email traffic or logging network access. Consequently, there is absolutely no motivation to combine these references.

The Office Action assertions that motivation exists because "Adolph is pertinent to the particular problem being solved in that it uses previous routes traveled to aid in further trips along the same route by storing previous routes and destinations traveled (FOA page 14, line 15) is simply not valid. Appellants disagree. More specifically, the problem addressed by *Andersen* is:

> the user, especially a knowledgeable computer user, could access the appropriate lists or records on his or her system and modify them to his or her own choosing. Thus, it would be beneficial to maintain a log of accesses to inappropriate systems, as well as possibly providing a way to prohibit access to such systems, which would be inaccessible to a system user.

(Column 1, line 31). The problem addressed by *Shipp* is "reduc[ing] the problem of dealing with new viruses borne by email" (page 2, line 10). Conversely however, the problem addressed by *Adolph* is:

> Since the known methods and systems only have subsets of the actual route network available, the route recommendations might involve considerable detours (with respect to length and time)... The effect of driving along detours can easily take on considerable significance considering that this fault applies to all mobile units [vehicles].

(Column 3, line 26). As is clearly evident from these passages, the problems addressed by *Andersen* (related to access of data by a computer user) and *Shipp* (related to email virus protection) are clearly and markedly different than the problem addressed by *Adolph* (related to vehicle routing). Consequently, a combination of these references is improper under the well established principles of *KSR*, as well as other applicable law.

For at least these reasons, the rejection that includes *Shipp*, *Andersen*, and *Adolph* is improper. Accordingly, Appellants respectfully request removal of this rejection and allowance of claim 1.

2. Claim 29 is Allowable Over *Andersen, Shipp,* and *Adolph*

The Office Action indicates that claim 29 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp* and *Adolph* fail to disclose, teach, or suggest all of the elements of claim 29. More specifically, claim 29 recites:

> A method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host:
>
> over the course of a first time interval, monitoring creation of sockets within the fist host to identify destination hosts identified therein;
>
> ***comparing identities of destination hosts monitored during the first time interval with destination host identities in a record***; and
>
> ***storing data from all sockets which identify monitored destination hosts not in the record***.
>
> ***(Emphasis added).***

Appellants respectfully submit that claim 29 is allowable over the cited art for at least the reason that none of *Andersen*, *Shipp*, and *Adolph*, taken alone or in combination, discloses, teaches, or suggests a "method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host... ***comparing identities of destination hosts monitored during the first time interval with destination host identities in a record***... [and] ***storing data from all sockets which identify monitored destination hosts not in the record***" as recited in claim 29. First, as previously argued, the combination of references simply does not teach "***storing data from all sockets which identify monitored destination hosts not in the record***." The Office Action has repeatedly argued that *Shipp* and *Andersen* must be considered. Appellants submit that even a combination of *Shipp* and *Andersen* fails to render claim 29 obvious. More specifically, *Shipp* clearly discloses a "logger 22 [that] is programmed so that the system logs components of each message so that similar messages can be detected. The following are logged: Subject line and digest of subject line; First few characters of text part of email, digest of first text part, and digest of first few characters..." (page 10, line 21). *Shipp* continues, disclosing:

> [t]he stopper 25 takes signatures from the searcher 24. The signature identifies characteristics of emails which must be stopped. On receiving the signature, all future matching emails are treated as viruses, and stopped. Obviously, the stopping action can take a number of forms, including... Holding them in temporary storage and

> notifying the addressee by email that an infected message has been intercepted and is being held for a period for their retrieval, should they wish, otherwise it will be deleted.

(Page 11, line 30).

As clearly illustrated in this passage, *Shipp* is identifying characteristics of the email message to determine whether to "hold them in temporary storage." *Andersen* however, discloses an "identifier of the host system being accessed, for example the URL of the host system being accessed, may be extracted from the request and be included as the log data to be forwarded to log server 150 of FIG. 1" (column 5, line 19). Because *Shipp* is clearly and exclusively identifying characteristics of the email message to determine whether to "hold them in temporary storage," *Shipp* has no use for an extracted URL, as disclosed in *Andersen*. Consequently, the combination of references could not have suggested the teachings of claim 29.

Similarly, the cited references fail to suggest "***comparing identities of destination hosts monitored during the first time interval with destination host identities in a record***" as recited in claim 29. More specifically, the Office Action admits "[t]he combination [of *Andersen* and *Shipp*] does not explicitly disclose establishing a record which is at least indicative of identities of hosts within the network to whom data has been sent by a first host" (OA page 4, line 18). Additionally, *Adolph* fails to overcome this deficiency. More specifically, *Adolph* discloses "[g]eneration of data by mobile units (vehicles) to model reality concerning route(s) and traffic and storing this data for further use" (Abstract). The portion of *Adolph* cited by the Office action includes citation of Denmark Patent No. 38 28 725 A1, which describes "a method to record and sort a route carried out for the first time with a facility installed in the subject vehicle" (column 1, line 40). As illustrated in this passage, *Adolph* does not even suggest a "method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host... ***comparing identities of***

destination hosts monitored during the first time interval with destination host identities in a record' as recited in claim 29.

Further, *Adolph* discloses a "method and device for generating, merging, and updating of destination [vehicle] traffic data" (title), which is completely different than a "method and apparatus for remote network access logging and reporting" (*Andersen* title) or "monitoring e-mail traffic for viruses" (*Shipp* title). More specifically, monitoring traffic data has nothing to do with monitoring email traffic or logging network access. Consequently, there is absolutely no motivation to combine these references.

The Office Action assertions that motivation exists because "Adolph is pertinent to the particular problem being solved in that it uses previous routes traveled to aid in further trips along the same route by storing previous routes and destinations traveled (FOA page 14, line 15) is simply not valid. Appellants disagree. More specifically, the problem addressed by *Andersen* is:

> the user, especially a knowledgeable computer user, could access the appropriate lists or records on his or her system and modify them to his or her own choosing. Thus, it would be beneficial to maintain a log of accesses to inappropriate systems, as well as possibly providing a way to prohibit access to such systems, which would be inaccessible to a system user.

(Column 1, line 31). The problem addressed by *Shipp* is "reduc[ing] the problem of dealing with new viruses borne by email" (page 2, line 10). Conversely however, the problem addressed by *Adolph* is:

> Since the known methods and systems only have subsets of the actual route network available, the route recommendations might involve considerable detours (with respect to length and time)... The effect of driving along detours can easily take on considerable significance considering that this fault applies to all mobile units [vehicles].

(Column 3, line 26). As is clearly evident from these passages, the problems addressed by *Andersen* (related to access of data by a computer user) and *Shipp*

(related to email virus protection) are clearly and markedly different than the problem addressed by *Adolph* (related to vehicle routing). Consequently, a combination of these references is improper under the well established principles of *KSR*, as well as other applicable law.

For at least these reasons, the rejection that includes *Shipp*, *Andersen*, and *Adolph* is improper. Accordingly, Appellants respectfully request removal of this rejection and allowance of claim 29.

3. Claim 43 is Allowable Over *Andersen, Shipp,* and *Adolph*

The Office Action indicates that claim 43 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp* and *Adolph* fail to disclose, teach, or suggest all of the elements of claim 43. More specifically, claim 43 recites:

> A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:
>
> ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;***
>
> during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;
>
> transmitting all requests to send data; and
>
> ***based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record.***

(Emphasis added).

Appellants respectfully submit that claim 43 is allowable over the cited art for at least the reason that none of *Andersen*, *Shipp*, and *Adolph*, taken alone or in combination, discloses, teaches, or suggests a "method of monitoring propagation of

viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host... ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***... [and] ***based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record***" as recited in claim 43. First, as previously argued, the combination of references simply does not teach "***based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record***." The Office Action has repeatedly argued that *Shipp* and *Andersen* must be considered. Appellants submit that even a combination of *Shipp* and *Andersen* fails to render claim 43 obvious. More specifically, *Shipp* clearly discloses a "logger 22 [that] is programmed so that the system logs components of each message so that similar messages can be detected. The following are logged: Subject line and digest of subject line; First few characters of text part of email, digest of first text part, and digest of first few characters..." (page 10, line 21). *Shipp* continues, disclosing:

> [t]he stopper 25 takes signatures from the searcher 24. The signature identifies characteristics of emails which must be stopped. On receiving the signature, all future matching emails are treated as viruses, and stopped. Obviously, the stopping action can take a number of forms, including... Holding them in temporary storage and notifying the addressee by email that an infected message has been intercepted and is being held for a period for their retrieval, should they wish, otherwise it will be deleted.

(Page 11, line 30).

As clearly illustrated in this passage, *Shipp* is identifying characteristics of the email message to determine whether to "hold them in temporary storage." *Andersen* however, discloses an "identifier of the host system being accessed, for example the URL of the host system being accessed, may be extracted from the request and be included as the log data to be forwarded to log server 150 of FIG. 1" (column 5, line 19).

Because *Shipp* is clearly and exclusively identifying characteristics of the email message to determine whether to "hold them in temporary storage," *Shipp* has no use for an extracted URL, as disclosed in *Andersen*. Consequently, the combination of references could not have suggested the teachings of claim 43.

Similarly, the cited references fail to suggest "***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***" as recited in claim 43. More specifically, the Office Action admits "[t]he combination [of *Andersen* and *Shipp*] does not explicitly disclose establishing a record which is at least indicative of identities of hosts within the network to whom data has been sent by a first host" (OA page 4, line 18). Additionally, *Adolph* fails to overcome this deficiency. More specifically, *Adolph* discloses "[g]eneration of data by mobile units (vehicles) to model reality concerning route(s) and traffic and storing this data for further use" (Abstract). The portion of *Adolph* cited by the Office action includes citation of Denmark Patent No. 38 28 725 A1, which describes "a method to record and sort a route carried out for the first time with a facility installed in the subject vehicle" (column 1, line 40). As illustrated in this passage, *Adolph* does not even suggest a "method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host... ***establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host***" as recited in claim 43.

Further, *Adolph* discloses a "method and device for generating, merging, and updating of destination [vehicle] traffic data" (title), which is completely different than a "method and apparatus for remote network access logging and reporting" (*Andersen* title) or "monitoring e-mail traffic for viruses" (*Shipp* title). More specifically, monitoring traffic data has nothing to do with monitoring email traffic or logging network access. Consequently, there is absolutely no motivation to combine these references.

The Office Action assertions that motivation exists because "Adolph is pertinent to the particular problem being solved in that it uses previous routes traveled to aid in further trips along the same route by storing previous routes and destinations traveled (FOA page 14, line 15) is simply not valid. Appellants disagree. More specifically, the problem addressed by *Andersen* is:

> the user, especially a knowledgeable computer user, could access the appropriate lists or records on his or her system and modify them to his or her own choosing. Thus, it would be beneficial to maintain a log of accesses to inappropriate systems, as well as possibly providing a way to prohibit access to such systems, which would be inaccessible to a system user.

(Column 1, line 31). The problem addressed by *Shipp* is "reduc[ing] the problem of dealing with new viruses borne by email" (page 2, line 10). Conversely however, the problem addressed by *Adolph* is:

> Since the known methods and systems only have subsets of the actual route network available, the route recommendations might involve considerable detours (with respect to length and time)... The effect of driving along detours can easily take on considerable significance considering that this fault applies to all mobile units [vehicles].

(Column 3, line 26). As is clearly evident from these passages, the problems addressed by *Andersen* (related to access of data by a computer user) and *Shipp* (related to email virus protection) are clearly and markedly different than the problem addressed by *Adolph* (related to vehicle routing). Consequently, a combination of these references is improper under the well established principles of *KSR*, as well as other applicable law.

For at least these reasons, the rejection that includes *Shipp*, *Andersen*, and *Adolph* is improper. Accordingly, Appellants respectfully request removal of this rejection and allowance of claim 43.

4. Claims 2 – 6, 8, 9, 14 – 18, 20, 21, 23, 28, 30 – 35, 38, 41, and 42 are Allowable Over *Andersen, Shipp,* and *Adolph*

The Office Action indicates that claims 2 – 6, 8, 9, 14 – 18, 20, 21, 23, 28, 30 – 35, 38, 41, and 42 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp* and *Adolph* fail to disclose, teach, or suggest all of the elements of claims 2 – 6, 8, 9, 14 – 18, 20, 21, 23, 28, 30 – 35, 38, 41, and 42. More specifically, dependent claims 2 – 6, 8, 9, 14 – 18, 20, 21, 23, and 28 are allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 1. Further, dependent claims 30 – 35, 38, 41, and 42 are allowable for at least the reason that they depend from and include the elements of allowable independent claim 29. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

5. Claim 7 is Allowable Over *Andersen, Shipp, Adolph,* and *Maher*

The Office Action indicates that claim 7 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*"), in view of U.S. Patent Number 7,058,974 ("*Maher*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp, Adolph,* and *Maher* fail to disclose, teach, or suggest all of the elements of claim 7. More specifically, dependent claim 7 is allowable for at least the reason that this claim depends from and includes the elements of allowable independent claim 1. Because *Maher* fails to overcome the deficiencies of *Andersen*, *Shipp*, and *Adolph*, claim 7 is

allowable as a matter of law. *In re Fine, Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

6. Claims 10 –13 and 24 – 27 are Allowable Over *Andersen, Shipp, Adolph,* and *Ramanujan*

The Office Action indicates that claims 10 – 13 and 24 – 27 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") U.S. Patent Number 5,341,491 ("*Ramanujan*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp, Adolph,* and *Ramanujan* fail to disclose, teach, or suggest all of the elements of claims 10 – 13 and 24 – 27. More specifically, dependent claims 10 – 13 and 24 – 27 are allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 1. Because *Ramanujan* fails to overcome the deficiencies of *Andersen*, *Shipp*, and *Adolph*, claims 10 – 13 and 24 – 27 are allowable as a matter of law. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

7. Claims 19 and 22 are Allowable Over *Andersen, Shipp, Adolph,* and *Cunningham*

The Office Action indicates that claims 19 and 22 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") E.P. Patent Number EP 0 986 229 ("*Cunningham*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp, Adolph,* and *Cunningham* fails to disclose, teach, or suggest all of the elements of claims 19 and 22. More specifically, dependent claims 19 and 22 are

allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 1. Because *Cunningham* fails to overcome the deficiencies of *Andersen*, *Shipp*, and *Adolph*, claims 19 and 22 are allowable as a matter of law. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

8. Claims 36, 37, 39, and 40 are Allowable Over *Andersen, Shipp, Adolph,* and *858*

The Office Action indicates that claims 36, 37, 39, and 40 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Number 6,122,740 ("*Andersen*"), in view of G.B. Patent Number GB 2 367 714 ("*Shipp*"), in view of U.S. Patent Number 6,356,836 ("*Adolph*") U.S. Patent Number 2002/0013858, Andersen ("*858*"). Appellants respectfully traverse this rejection for at least the reason that *Andersen* in view of *Shipp, Adolph,* and *858* fail to disclose, teach, or suggest all of the elements of claims 36, 37, 39, and 40. More specifically, dependent claims 36, 37, 39, and 40 are allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 29. Because *858* fails to overcome the deficiencies of *Andersen*, *Shipp*, and *Adolph*, claims 36, 37, 39, and 40 are allowable as a matter of law. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

VIII. Conclusion

In summary, the pending claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellants therefore respectfully request that the Board of Appeals overturn the Examiner's rejection and allow the pending claims.

Respectfully submitted,

By: 

Anthony F. Bonner, Jr.
Registration No. 55,012

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

transmitting all requests to send data; and

storing in a buffer data relating to requests which identify a destination host not in the record.

2. A method according to claim 1 wherein the record is established by monitoring identities of destination hosts to whom requests have been transmitted during a second time interval, which precedes the first time interval.

3. A method according to claim 2, wherein the record contains a predetermined maximum number of destination host identities, the maximum number being defined in accordance with a policy.

4. A method according to claim 3, wherein the policy additionally defines a maximum number of destination host identities not in the record, to whom requests may be legitimately transmitted in accordance with the policy.

5. A method according to claim 4 further comprising the step, at the end of any given time interval, of deleting from the buffer data relating to requests transmitted during the given time interval in accordance with the policy.

6. A method according to claim 5 further comprising the step, at the end of the given time interval, of updating the record to reflect identities of hosts identified in requests which are transmitted in accordance with the policy during the given time interval.

7. A method according to claim 6 further comprising the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with the policy.

8. A method according to claim 1, wherein the stored data is offered in the buffer and includes a copy of a socket created to send data in accordance with a request.

9. A method according to claim 8 wherein the socket enables identification of at least one application program at whose behest the socket is created.

10. A method according to claim 1 further comprising the steps of:

determining the value of parameter ("slack") based upon a number of successive time periods that pass when no new requests are made to send data from the first host to hosts not in the record; and

when slack exceeds a predetermined value, allowing un-impeded passage of data from the first host to destination hosts not in the record.

11. A method as claimed in claim 10, wherein slack is determined based upon the number of successive time periods for which the buffer is empty.

12. A method as claimed in claim 10, wherein slack has a predetermined maximum value.

13. A method as claimed in claim 10, wherein the value of slack is decremented each time an un-impeded passage of data from the first host to a destination host not in the record is allowed.

14. A method according to claim 10, wherein said time periods are of equal duration to at least one of said time intervals.

15. A method according to claim 1 further comprising the steps of monitoring the rate of increase in the size of the buffer, and

in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a virus warning.

16. A method according to claim 1 further comprising the steps of monitoring the increase in the size of the buffer per time interval, and

in the event that the increase in the size of the buffer in any given time interval exceeds a predetermined size, generating a virus warning.

17. A method according to claim 1 further comprising the steps of monitoring the size of the buffer, and

in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a virus warning.

18. A method as claimed in claim 1, further comprising the step of varying with time at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record.

19. A method as claimed in claim 18, wherein said at least one parameter is varied as a function of the time of day.

20. A method as claimed in claim 18, wherein said at least one parameter is varied in response to a perceived threat level.

21. A method as claimed in claim 18, wherein said at least one parameter is changed between a first set of values and a second set of values at a predetermined rate.

22. A method as claimed in claim 21, wherein at least one of the values of said at least one parameter is randomly changed according to a predetermined probability distribution as a function of time.

23. A method as claimed in claim 1, further comprising the step of determining at least one parameter that defines a state of viral infection and is selected from the group consisting of:

number of destination hosts in the record; and

threshold number of requests identifying destination hosts not in the record by performing an automated search on a set of data indicative of normal network traffic.

24. method according to claim 1 further comprising the steps of:

receiving a request to send a multiple recipient email from the first host;

determining the value of a parameter ("mslack") based upon the number of successive time periods that pass when no multiple recipient emails are sent from the first host;

if mslack exceeds a predetermined value, allowing un-impeded passage of the multiple recipient email.

25. A method according to claim 24, wherein the multiple recipient email is allowed un-impeded passage if mslack is greater than or equal to the number of intended recipients of the email.

26. A method as claimed in claim 24, wherein mslack is set to zero after the multiple recipient email has been sent.

27. A method as claimed in claim 24, wherein mslack has a predetermined maximum value.

28. A method according to claim 24, wherein said time periods are of equal duration to at least one of one or more time intervals.

29. A method of operating a first host within a network of a plurality of hosts, said method comprising the following steps carried out by a first host:

over the course of a first time interval, monitoring creation of sockets within the fist host to identify destination hosts identified therein;

comparing identities of destination hosts monitored during the first time interval with destination host identities in a record; and

storing data from all sockets which identify monitored destination hosts not in the record.

30. A method according to claim 29 wherein the stored socket data at least enables identification of the destination host identified therein.

31. A method according to claim 29 wherein the record identifies a maximum number of destination hosts, the maximum number being determined in accordance with a policy.

32. A method according to claim 31 wherein the record is established by monitoring creation of sockets during a time interval preceding the first time interval.

33. A method according to claim 31 wherein the policy additionally specifies a maximum number of sockets, each identifying a destination host not in the record, to be legitimately created in any given time interval.

34. A method according to claim 33 wherein at the end of a time interval, socket data containing identities of destination hosts in respect of whom sockets have legitimately been created is deleted.

35. A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host.

36. A method according to claim 35 wherein packets having a designated destination IP address are stored.

37. A method according to claim 36 further comprising the step of establishing the predetermined IP address from the stored socket data.

38. A method according to claim 29 further comprising the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing incoming packets to the first host.

39. A method according to claim 38 wherein packets having a designated source IP address are stored.

40. A method according to claim 39, further comprising the step of establishing the predetermined IP address from the stored socket data.

41. A method according to claim 29 wherein socket data is stored in a buffer.

42. A method according to claim 1, wherein the step of automatically transmitting all requests comprises transmitting the data related to the requests.

43. A method of monitoring propagation of viruses by a first host within a network of hosts, the method comprising the following steps carried out by the first host:

establishing a record which is at least indicative of identities of destination hosts within the network to whom data has been sent by the first host;

during a first time interval, comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record;

transmitting all requests to send data; and

based on the result of said comparing, storing in a buffer data to identify as such those requests which identify a destination host not in the record.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

(None)

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

(None)